CLAIMS 1, 3-12 and 16-33 DEFINE PATENTABLE SUBJECT MATTER PURSUANT TO U.S.C. §103

The Office Action rejects claim 1, 3-12 and 16-33 under 35 U.S.C. §103 U.S. Patent No. 6,971,028 to Lyle et al. (hereinafter "Lyle") in view of Botros et al. (hereinafter "Botros"). The rejection is respectfully traversed.

Lyle is directed to a system for tracking the source of computer attacks. Lyle relies upon receiving data that is associated with an attack and then associating that data with an event. According to Lyle, the data may be received from another administrative domain external to the network concerning an attack or potential attack that is being tracked by another administrative domain. Such data may be received: 1.) as an e-mail message received by a network security administrator providing information concerning the attack or suspected attack being experienced by another administrative domain; or 2.) from another administrative domain without human intervention in the form of a message received by a tracking system via its network connection containing information concerning the attack or suspected attack. The data requiring analysis and/or evaluation may also be received from a source internal to the administrative domain being served by the tracking system. In one embodiment, a "sniffer" module continuously scans the data being received at various ports of various network devices. The sniffers search for data indicating an actual or suspected attack and provide information concerning suspicious data to other modules within the tracking system. According to Lyle, data requiring further analysis is stored and placed in a queue for analysis by a tracking system. Responsive action may be taken based upon the analysis of the data.

Thus, the invention of Lyle provides for compiling a group of suspected attacks which are communicated to others and then analyzed. Thus, in Lyle, the analysis occurs after actions have been taken. In contrast to the Applicant's invention, there is no human behavior assessment capability provided in Lyle. For example, the system in Lyle does not convert packet level activity into human behaviors and activities for each IP/user or convert the sorted IP/user behavioral activities into behavioral measures of expertise and deception as measures of underlying intent for each IP/user as provided in claim 1 of the Applicant's invention.

Botros discloses a method and apparatus for training a neural network model for use in network intrusion detection. In Botros, an artificial set of features reflecting anomalous behavior for a particular activity is created. Then, a distribution of users of normal feature values and an expected distribution of users of anomalous feature values is then defined. Anomalous behavior feature values are then produced. Potential intrusions into the computer network can be detected by utilizing the artificially created anomalous behavior feature values. Thus, Botros provides an anomaly detection system. However, as with Lyle, Botros fails to provide real-time assessment of behavior characteristics. In contrast to the Applicant's invention, Botros requires samples of current activity on a specific network to differentiate between intrusive behavior and regular network activity.

The Applicant's invention provides a back propagation network (BPN) that provides a combined expertise and deception (E/D) rating for each single monitored behavior, as well as for specific combinations of monitored behaviors. The BPN in accordance with the invention is capable of providing the E/D combined rating for any possible combination of the behaviors monitored. As an example, if n = 200 monitored behaviors, the trained BPN can return E/D

determinations for all 2^{200} possible combinations of behaviors presented to the BPN at any given time sample for any given user. This feature of the present invention provides for E/D assessments that far exceed the relatively small number of examples used for training. This is in marked contrast to a prior art rule-based signature detection system whereby every determination made must be stated as a defined rule. If 200 rules are in effect, then only 200 determinations can be made with a signature detection system, whereas all exhaustive combinations of behaviors monitored by the present invention result in accurate E/D ratings equating to determinations of threat as opposed to detections following rules as in a signature detection system.

The invention should be contrasted with signature detection systems that are severely restricted by making a one to one correspondence between detections and a threat/no threat decision. The Applicant's invention, in contrast is capable of presenting the level of expertise and deception present for any given monitored behavior with all possible combinations of all other monitored behaviors. Because high E and High D assessments equate to threat and that such determinations can be made almost instantaneously across all possible exhaustive combinations of all monitored behaviors, the Applicant's invention covers the entire and exhaustive assessment space created by any and all combinations of behaviors monitored that could co-occur, even if a specific and rare combination of behaviors is presented to the BPN for the first time. A signature detection system, on the other hand, without a predefined rule for a new behavior of concern is not capable of detection of that new event.

Thus, the combination of Lyle and Botros fails to disclose the Applicant's invention which provides converting the sorted IP/user behavioral activities into behavioral measures of expertise and deception as measures of underlying intent for each IP/user in order to generate an

assessment, wherein the assessment is made for every possible combination of behaviors and activities whether or not such behaviors and activities have been previously encountered, as recited in claim 1. As described above, neither Lyle nor Botros can assess every possible monitored rule or pattern using human behavioral assessment measures to determine the degree of expertise and deception present in any given sample of IP/User behavior. Furthermore, neither Lyle or Botros provide the requisite motivation to combine and modify their teachings to arrive at the Applicant's invention as claimed in claim 1. Therefore withdrawal of the rejection of claim 1 under 35 U.S.C 103 is respectfully requested. Withdrawal of the rejection of dependant claims 3-11 is requested for the reasons described above and for the additional features that they recite.

With regard to claims 12, respectfully submits that the points raised above in connection with claim 1 are equally applicable. Thus, Lyle and Botros fail to disclose or suggest, an outcome director operatively coupled to the inter-port fusion monitor that determines whether to block or track IP/users on a specific IP/User basis based upon assessed behavioral measures of intent, wherein the assessed behavioral measure of intent are made for every possible combination of behaviors and activities whether or not such combinations behaviors and activities have been previously encountered, as recited in claim 12. Thus, withdrawal of the rejection of claim12 and dependant claims 16-29, 32 and 33. is respectfully requested.

With regard to claim 30, respectfully submits that the points raised above in connection with claim 1 are equally applicable. Thus, Lyle and Botros fail to disclose or suggest a first conversion means for converting packet level activity into human behaviors and activities for each IP/user, including assigning a binary representation (1=present, 0=absent) to each human

behavior and activity and a second conversion means for converting the IP/User specific activities/behaviors to behavioral measures of expertise and deception as measures of underlying intent for each IP/user in order to generate an assessment, wherein the assessment is made for every possible combination of behaviors and activities whether or not such combinations behaviors and activities have been previously encountered, as recited in claim 30. Thus, withdrawal of the rejection of claim 30 is respectfully requested.

With regard to claim 31, respectfully submits that the points raised above in connection with claim 1 are equally applicable. Thus, Lyle and Botros fail to disclose or suggest computer readable program code configured to cause the computer to covert the packet level activity into human behaviors and activities for each IP/user and convert the sorted IP/user behavioral activities into behavioral measures of expertise and deception as measures of underlying intent for each IP/user in order to generate an assessment, wherein the assessment is made for every possible combination of behaviors and activities whether or not such combinations behaviors and activities have been previously encountered, as recited in claim 31. Thus, withdrawal of the rejection of claim 30 is respectfully requested.

CONCLUSION

In view of the foregoing, Applicant respectfully requests reconsideration and the allowance of the above-identified application. Should the Examiner feel that there are any issues outstanding after consideration of this response, the Examiner is invited to contact Applicant's representative at the telephone number listed below.

If there are any other fees due in connection with the filing of this response, please charge the fees to our Deposit Account No. 50-1349. If a fee is required for an extension of time under

37 C.F.R. § 1.136 not accounted for above, such an extension is requested and the fee should also be charged to our Deposit Account.

Respectfully submitted,

Dated: December 14, 2006

Ajit J. Vaidya
Registration No. 43,214

HOGAN & HARTSON LLP
555 13th Street, N.W.
Washington, D.C. 20004
(202) 637-5600
Customer No.: **24633**